69

No. (1)

Supreme Court, U.S.
FILED
07-496 OCT 10 2007
OFFICE OF THE CLERK

In The

Supreme Court of the United States

JEROME T. HECKENKAMP,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of *Certiorari*
To The United States Court Of Appeals
For The Ninth Circuit

PETITION FOR A WRIT OF *CERTIORARI*

BENJAMIN L. COLEMAN
COLEMAN & BALOGH LLP
433 G Street, Suite 202
San Diego, California 92101
Telephone (619) 652-9960

Attorneys for Petitioner

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

QUESTION PRESENTED

Whether the "special needs" exception established by the Court in *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), which allows warrantless searches of juveniles in the elementary and secondary school contexts, applies to non-programmatic searches of adult students in the university context.

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	iii
OPINION BELOW	1
JURISDICTION	1
CONSTITUTIONAL PROVISION	1
STATEMENT OF THE CASE	1
ARGUMENT	10
CONCLUSION	15
APPENDIX	App. 1
Opinion Below	App. 1
Order Denying Rehearing	App. 17

TABLE OF AUTHORITIES

Page

CASES

Anobile v. Pelligrino, 303 F.3d 107 (2d Cir. 2002) 14

Board of Education of Independent School District No. 92 of Pottawatomie County v. Earls, 536 U.S. 822 (2002) 11

Brigham City, Utah v. Stuart, 126 S. Ct. 1943 (2006) 14

Chandler v. Miller, 520 U.S. 305 (1997) 12

City of Indianapolis v. Edmond, 531 U.S. 32 (2000) 12

Ferguson v. City of Charleston, 532 U.S. 67 (2001) 11, 12

Griffin v. Wisconsin, 483 U.S. 868 (1987) 12

Marks v. United States, 430 U.S. 188 (1977) 13

Murray v. United States, 487 U.S. 533 (1988) 15

National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989) 12

New Jersey v. T.L.O., 469 U.S. 325 (1985) 9, 10, 11, 12, 13

O'Connor v. Ortega, 480 U.S. 709 (1987) 12, 13, 14

Piazzola v. Watkins, 442 F.2d 284 (5th Cir. 1971) 14

Skinner v. Railway Labor Executives Association, 489 U.S. 602 (1989) 12

TABLE OF AUTHORITIES – Continued

Page

Steagald v. United States, 451 U.S. 204 (1981) 15

United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007) ..... *passim*

Vernonia School District 47J v. Acton, 515 U.S. 646 (1995) 12

Washington v. Chrisman, 455 U.S. 1 (1982) 14

CONSTITUTION

U.S. Const. amend. IV ..... *passim*

STATUTES

18 U.S.C. § 1030 8

18 U.S.C. § 3231 8

28 U.S.C. § 1254 1

RULES

S. Ct. R. 10 10

OPINION BELOW

The opinion below is published at *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007).

JURISDICTION

The opinion of the court of appeals was filed on April 5, 2007. The court of appeals denied a petition for rehearing and rehearing *en banc* on July 19, 2007. The Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION

The Fourth Amendment provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the places to be searched, and the persons or things to be seized."

U.S. Const. amend. IV.

STATEMENT OF THE CASE

The following text is mostly a verbatim recitation of the background contained in the court of appeals' opinion. *See Heckenkamp*, 482 F.3d at 1143-46. Some

of the inaccuracies and incomplete information in the lower court's statement of the case is noted in footnotes.

In December 1999, Scott Kennedy, a computer system administrator for Qualcomm Corporation in San Diego, California, discovered that somebody had obtained unauthorized access to (or "hacked into," in popular parlance) the company's computer network. Kennedy contacted Special Agent Terry Rankhorn of the Federal Bureau of Investigation about the intrusion.

Kennedy was able to trace the intrusion to a computer on the University of Wisconsin at Madison network, and he contacted the university's computer help desk, seeking assistance. Jeffrey Savoy, the University of Wisconsin computer network investigator, responded to Kennedy's request and began examining the university's system.[1] Savoy found evidence that someone using a computer on the university network was in fact hacking into the Qualcomm system and that the user had gained unauthorized access to the university's system as well. Savoy was particularly concerned that the user had gained

---

[1] The lower court stated that Savoy "promptly" responded. *Heckenkamp*, 482 F.3d at 1143. More precisely, the Qualcomm administrator contacted the computer staff at the university on December 7, 1999. The Qualcomm administrator was informed that he would have to wait until the next day to speak with the appropriate person. Savoy then responded the next day, December 8, 1999. In other words, this was not treated like an emergency situation.

access to the "Mail2" server on the university system, which housed accounts for 60,000 individuals on campus and processed approximately 250,000 emails each day. At that time, students on campus were preparing for final exams, and Savoy testified that "the disruption on campus would be tremendous if e-mail was destroyed." Through his investigation of the Mail2 server, Savoy identified a computer located in university housing as possibly being involved.[2] The type of access the user had obtained was restricted to specific system administrators.

Savoy had determined that the identified computer in university housing had an Internet Protocol ("IP") address that ended in 117. In addition, Savoy determined that petitioner, who was a computer science graduate student at the university, had checked his email from that IP address 20 minutes before and 40 minutes after the unauthorized connections between the computer at the IP address ending in 117, the Mail2 server, and the Qualcomm server. Savoy determined that the computer at the IP address had been used regularly to check petitioner's email account, but no others. Savoy became extremely concerned because he knew that petitioner had been terminated from his job at the university

[2] The lower court stated that Savoy traced the "source" of the hacking to this particular computer located in university housing. *Heckenkamp*, 482 F.3d at 1144. In actuality, the mail server was being used to access this computer, which indicated that the computer may have been the victim of hacking, not the "source" of the hacking.

computer help desk two years earlier for unauthorized activity, and Savoy knew that petitioner "had technical expertise to damage the university's system."

Savoy checked housing records to ensure that the IP address was assigned to petitioner's dorm room. However, the housing department stated that the IP address did not correspond with petitioner's room and instead corresponded with a room in a different dormitory.[3] The housing department acknowledged that the records could be inaccurate but stated that they would not be able to verify the location of the IP address until the next morning. In order to protect the university's server, Savoy electronically blocked the connection between IP address 117 and the Mail2 server.

After blocking the connection, Savoy contacted Rankhorn. After Savoy informed Rankhorn of the information he had found, Rankhorn told Savoy that he intended to get a warrant for the computer, but he did not ask Savoy to take any action or to commence any investigation.[4]

---

[3] The lower court stated that the two rooms were "down the hall" from each other. *Heckenkamp*, 482 F.3d at 1144. Petitioner lived in Room 107 of Noyes House. The housing records showed that the 117 address was located in Room 115 of Siebecker House.

[4] Actually, Savoy communicated with Detective Doug Scheller, of the university's police department, in order to determine how to proceed. Scheller in turn contacted Agent Rankhorn and asked

(Continued on following page)

Later that night, Savoy decided to check the status of the 117 computer from home because he was still concerned about the integrity of the university's system. He logged into the network and determined that the 117 computer was not attached to the network. Savoy was still concerned that the same computer could have "changed its identity," so he checked the networking hardware to determine if the computer that was originally logged on at the 117 address was now logged on at a different IP address. His search confirmed that the computer was now logged on at an IP address ending in 120.

Savoy then decided to hack into the computer that was logged on at the 120 address by using a name and password that he had discovered in his investigation.[5] Savoy used a series of commands to confirm that the 120 computer was the same

---

him to call Savoy so that they could all form a plan of action. At approximately 3:00 p.m. on December 8, Rankhorn contacted Savoy, and they determined that the best course of action was to arrange for an FBI agent to interview petitioner the next day.

[5] The lower court stated that Savoy took this step because he was concerned for the security of Mail2 and was worried that the suspected intruder would know that he was being investigated. In actuality, an intruder would not have known that he was being investigated until *after* Savoy hacked into the computer. Moreover, the lower court opinion omits that Savoy admitted to hacking into the computer "to gather evidence of possible hacking activity." Savoy further admitted that he accessed the computer because he "wanted to positively identify the computer using the aforementioned [117 and 120] IP addresses and to gather any evidence of a break-in."

computer that had been logged on at 117 and to determine whether the computer still posed a risk to the university server. After approximately 15 minutes of looking only in the temporary directory, without deleting, modifying, or destroying any files, Savoy logged off of the computer.[6]

Savoy then determined that "the 120 machine needed to get off line immediately or as soon as possible" based on "a university security need." He contacted both Rankhorn and Detective Scheller. Savoy informed them of his discoveries and concerns. Rankhorn asked Savoy to wait to take action because he was attempting to get a search warrant. However, Savoy felt that he needed to protect the university's system by taking the machine off line immediately. Therefore, he made the decision to coordinate with the university police to take the computer off line and to "let the university police coordinate with the FBI."

Together with Scheller and other university police officers, Savoy went to the room assigned to petitioner. Nobody was in the room when they arrived. Savoy and

---

[6] The lower court's description of Savoy's search of the computer was inaccurate and incomplete. During the search, Savoy "observed what he believed was evidence of hacker programs residing in that particular directory [and] he then ran further commands to gather evidence." Consistent with his investigative motivations, Savoy searched petitioner's computer with a series of commands designed to locate particular source codes that were so important to his investigation that "he made screen print copies of these files as evidence." Savoy's search also revealed that the computer did belong to petitioner.

Scheller entered the room and disconnected the network cord attaching the computer to the network. Savoy noted that the computer had a screen saver with a password, which prevented him from accessing the computer. In order to be sure that the computer he had disconnected from the network was the computer that had gained unauthorized access to the Mail2 server, Savoy wanted to run some commands on the computer. Detective Scheller located petitioner, explained the situation and asked for petitioner's password, which petitioner provided.

Savoy used the password to run the commands on the computer and verified that it was the computer used to gain the unauthorized access. After Savoy confirmed that he had the right computer, Scheller advised petitioner that he was not under arrest, but Scheller requested that petitioner waive his *Miranda* rights and give a statement. Petitioner waived his rights in writing and answered the investigator's and detectives' questions. In addition, petitioner authorized Savoy to make a copy of his hard drive for later analysis, which Savoy did. At no time did Savoy or Scheller search petitioner's room. Throughout his testimony, Savoy emphasized that his actions were taken to protect the university's server rather than for law enforcement purposes.[7]

---

[7] Savoy, however, stated that he enlisted the help of the university police so that he could "secure the evidence" on petitioner's computer. Furthermore, as the Ninth Circuit recognized, Savoy came to petitioner's room armed with equipment to mirror

(Continued on following page)

The federal agents obtained a search warrant from the Western District of Wisconsin, which was executed later in the day. Pursuant to the warrant, the agents seized the computer and searched petitioner's room.

Petitioner was indicted in both the Northern and Southern Districts of California on multiple offenses, including counts of recklessly causing damage by intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(B).[8] In separate orders, Judge Ware in the Northern District and Judge Jones in the Southern District denied petitioner's motions to suppress the evidence gathered from (1) the remote search of his computer, (2) the image taken of his computer's hard drive, and (3) the search conducted pursuant to the FBI's search warrant. The two cases were eventually consolidated before Judge Ware, and petitioner entered a conditional guilty plea to two counts of violating section 1030(a)(5)(B), which allowed him to appeal the denials of his motions to suppress.

The Ninth Circuit affirmed. The court of appeals first held that petitioner had a reasonable expectation of privacy in his dorm room computer. *See Heckenkamp*, 482 F.3d at 1146-47. However, relying on

---

petitioner's hard drive, demonstrating his mission to gather evidence and not simply protect the university system.

[8] The district court asserted jurisdiction pursuant to 18 U.S.C. § 3231.

concurring opinions in *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), the lower court found that Savoy's remote search of petitioner's computer was justified under the special needs exception to the Fourth Amendment's warrant requirement. *See Heckenkamp*, 482 F.3d at 1147-48.[9] The Ninth Circuit reasoned: "Just as requiring a warrant to inv stigate potential drug use would disrupt operations of a high school, *see T.L.O.*, 469 U.S. at 352-53 (Blackmun, J., concurring in the judgment), requiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function."

[9] In doing so, the Ninth Circuit noted that "[u]nder the university's policies, to which [petitioner] assented when he connected his computer to the university's network, Savoy was authorized to 'rectify emergency situations that threaten the integrity of campus computer or communication systems, provided that use of accessed files is limited solely to maintaining or safeguarding the system.'" *Heckenkamp*, 482 F.3d at 1147-48. The Ninth Circuit incorrectly quoted a supposed policy governing university-owned computers used by the faculty in their offices, which was obviously inapplicable to petitioner's personally owned dorm room computer. Indeed, the policy specifically stated it did "not address how departments and schools may access students' instructional accounts" and that it only governed university-owned computers used by "[t]he faculty and staff of the University" at their work stations. The supposed policy cited by the Ninth Circuit did not in any way govern petitioner's personally owned dorm room computer.

Heckenkamp, 482 F.3d at 1148 (parallel citations omitted).[10]

ARGUMENT

In finding that a state university official's remote search of petitioner's dorm room computer did not require a warrant, the Ninth Circuit became the first federal court of appeals to extend the Fourth Amendment's "special needs" exception to the university setting. Yet, the only authority relied upon by the lower court, concurring opinions in the Court's seminal decision in *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), *see Heckenkamp*, 482 F.3d at 1148, specifically limits the applicability of the special needs exception to the elementary and secondary school contexts. The lower court's departure from the very precedent that it cites has the potential to affect tens of thousands of state university students in the Ninth Circuit. In short, the Ninth Circuit has decided an important federal question in a way that conflicts with relevant decisions of the Court, and therefore the instant petition should be granted. *See* S. Ct. R. 10.

[10] The Ninth Circuit also assumed that the subsequent warrantless search of petitioner's dorm room violated the Fourth Amendment but that the evidence obtained from that search was nonetheless admissible under the independent source exception to the exclusionary rule. *See Heckenkamp*, 482 F.3d at 1148-49. The Ninth Circuit's independent source finding was predicated on its finding that Savoy's remote search of petitioner's computer was constitutional.

In *T.L.O.*, the Court held that a warrantless search of a public high school student's purse by an assistant principal complied with the Fourth Amendment. Writing for a three-member plurality, Justice White held that public school officials can search students and their effects without a warrant or probable cause as long as the search is reasonable. *See T.L.O.*, 469 U.S. at 341. In a separate concurring opinion, Justice Blackmun explained that "[o]nly in those exceptional circumstances in which *special needs*, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers." *Id.* at 351 (emphasis added). He concluded that "[t]he elementary and secondary school setting presents a *special need* for flexibility justifying a departure from the balance struck by the Framers." *Id.* at 352 (emphasis added).

The language used by Justice Blackmun spawned the so-called "special needs" exception to the Fourth Amendment's warrant and probable cause requirements. Since *T.L.O.*, the Court has frequently applied the exception in the context of *programmatic* searches, typically drug testing programs instituted by public officials. *See Board of Education of Independent School District No. 92 of Pottawatomie County v. Earls*, 536 U.S. 822 (2002) (drug testing program of high school students participating in competitive extracurricular activities upheld); *Ferguson v. City of Charleston*, 532 U.S. 67 (2001) (drug

testing program of pregnant women struck down); *Chandler v. Miller*, 520 U.S. 305 (1997) (drug testing program of candidates for state office struck down); *Vernonia School District 47J v. Acton*, 515 U.S. 646 (1995) (drug testing program of high school student athletes upheld); *Skinner v. Railway Labor Executives Association*, 489 U.S. 602 (1989) (drug testing program of railroad employees upheld); *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989) (drug testing program of customs employees upheld); *see also Griffin v. Wisconsin*, 483 U.S. 868 (1987) (state regulatory scheme authorizing warrantless searches of probationers upheld).[11]

While the Court has frequently applied the special needs exception in the context of *programmatic* searches, it has only applied the exception on one occasion since *T.L.O.* in the context of an *individualized* search. In *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Court, in a plurality opinion, held that a warrantless search of a state employee's office was permissible under the special needs exception. The

---

[11] In evaluating the legitimacy of these searches, the purpose of the program has generally been the decisive factor. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 45-46 (2000) ("programmatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion"). Thus, in *Ferguson*, the drug testing program was struck down because its purpose was intertwined with law enforcement; similarly, in *Chandler*, the drug testing program was struck down because there was not a particularly "special" need for the program. *See Ferguson*, 532 U.S. at 79-81.

opinions in *O'Connor* and *T.L.O.*, however, do not support extending the special needs exception to non-programmatic searches of university students.[12]

In *T.L.O.*, the decisive factor permitting the individualized search was the specific context of educating *juveniles*. The concurring opinions of Justices Powell (joined by Justice O'Connor) and Blackmun, which should be viewed as the controlling rule of law for the 3-2-1-3 decision, *see Marks v. United States*, 430 U.S. 188, 193 (1977), both emphasized that the special needs exception for such searches was limited to the elementary and secondary school context. *See T.L.O.*, 469 U.S. at 348, 352-53. Indeed, Justice Powell began his concurring opinion by emphasizing "the special characteristics of elementary and secondary schools that make it unnecessary to afford students the same constitutional protections granted adults and juveniles in a nonschool setting." *Id.* at 348. Put simply, the special need to eliminate Fourth Amendment requirements that exists in the educational setting for juveniles does not carry over to adult education, nor has the Court ever suggested such an extension.

Similarly, the Court's reliance on the special needs exception to justify the non-programmatic

---

[12] This case only requires the Court to consider whether the special needs exception applies to *individualized* searches in the university setting; the Court need not determine whether the exception justifies *programmatic* searches in the university setting, such as drug testing for athletes at state universities.

search of the public employee's office in *O'Connor* does not support application of that doctrine in this context. In arriving at its conclusion, the plurality opinion in *O'Connor* explained: "Balanced against the substantial government interests in the efficient and proper operation of the workplace are the privacy interests of government employees in their place of work which, while not insubstantial, are far less than those found at home or in some other contexts." *O'Connor*, 480 U.S. at 725. Unlike the workplace, many students in the university setting, such as petitioner in this case, live in dormitories and other types of university housing, and the Court has previously assumed that a university student's dormitory room is the equivalent of his home for Fourth Amendment purposes. *See Washington v. Chrisman*, 455 U.S. 1 (1982); *see also Anobile v. Pelligrino*, 303 F.3d 107, 119-20 (2d Cir. 2002); *Piazzola v. Watkins*, 442 F.2d 284, 289-90 (5th Cir. 1971). In short, the university student's privacy interests in his dorm room are certainly more substantial than a public employee's privacy interest in his office.

Finally, the lower court's unprecedented and unexplained extension of the special needs exception to the university setting is perplexing because there is a well-established Fourth Amendment doctrine that governs the circumstances of this case. Specifically, the exigent circumstances exception allows officials to conduct searches without a warrant in certain emergency situations. *See, e.g., Brigham City, Utah v. Stuart*, 126 S. Ct. 1943, 1947-49 (2006). The

Ninth Circuit may have ignored the exigent circumstances exception, despite petitioner's insistence that the constitutionality of the search should be assessed under that doctrine, because the government refused to rely on exigent circumstances as a justification for the search.[13] By taking this approach, however, the government and the Ninth Circuit have improperly extended the special needs doctrine to the university context in contravention of the Court's precedent. As a result, the instant petition should be granted to correct this erroneous extension.

CONCLUSION

For the foregoing reasons, the Court should grant the instant petition for a writ of *certiorari*.

Respectfully submitted,

Dated: October 10, 2007

BENJAMIN L. COLEMAN
COLEMAN & BALOGH LLP
433 G Street, Suite 202
San Diego, California 92101
Telephone (619) 652-9960

Attorneys for Petitioner

[13] Whether the government thereby waived the claim, *see Steagald v. United States*, 451 U.S. 204, 208-11 (1981), and whether the circumstances constituted an emergency that would trigger the exigent circumstances doctrine are questions that should be left for the lower courts in the first instance. *See, e.g., Murray v. United States*, 487 U.S. 533, 543-44 (1988).

482 F.3d 1142

United States Court of Appeals, Ninth Circuit.
UNITED STATES of America, Plaintiff-Appellee,
v.
Jerome T. HECKENKAMP, Defendant-Appellant.
United States of America, Plaintiff-Appellee,
v.
Jerome T. Heckenkamp, Defendant-Appellant.
Nos. 05-10322, 05-10323.

Argued and Submitted Aug. 17, 2006.
Filed April 5, 2007.

Benjamin Coleman, San Diego, CA, for the appellant.

Hanley Chew, Assistant United States Attorney, San Francisco, CA, for the appellee.

Appeal from the United States District Court for the Northern District of California; James Ware, District Judge, Presiding. D.C. Nos. CR-03-20041-JW, CR-00-20355-JW.

Before CANBY, HAWKINS, and THOMAS, Circuit Judges.

THOMAS, Circuit Judge.

In this case, we consider whether a remote search of computer files on a hard drive by a network administrator was justified under the "special needs" exception to the Fourth Amendment because the administrator reasonably believed the computer had been used to gain unauthorized access to confidential

records on a university computer. We conclude that the remote search was justified.

Although we assume that the subsequent search of the suspect's dorm room was not justified under the Fourth Amendment, we conclude that the district court's denial of the suppression motion was proper under the independent source exception to the exclusionary rule.

I

In December 1999, Scott Kennedy, a computer system administrator for Qualcomm Corporation in San Diego, California, discovered that somebody had obtained unauthorized access to (or "hacked into," in popular parlance) the company's computer network. Kennedy contacted Special Agent Terry Rankhorn of the Federal Bureau of Investigation about the intrusion.

Kennedy was able to trace the intrusion to a computer on the University of Wisconsin at Madison network, and he contacted the university's computer help desk, seeking assistance. Jeffrey Savoy, the University of Wisconsin computer network investigator, promptly responded to Kennedy's request and began examining the university's system. Savoy found evidence that someone using a computer on the university network was in fact hacking into the Qualcomm system and that the user had gained unauthorized access to the university's system as well. Savoy was particularly concerned that the user had gained access to the "Mail2" server on the university system, which housed

accounts for 60,000 individuals on campus and processed approximately 250,000 emails each day. At that time, students on campus were preparing for final exams, and Savoy testified that "the disruption on campus would be tremendous if e-mail was destroyed." Through his investigation of the Mail2 server, Savoy traced the source of intrusion to a computer located in university housing. The type of access the user had obtained was restricted to specific system administrators, none of whom would be working from the university's dormitories.

Savoy determined that the computer that had gained unauthorized access had a university Internet Protocol ("IP") address[1] that ended in 117. In addition, Savoy determined that Heckencamp, who was a computer science graduate student at the university, had checked his email from that IP address 20 minutes before and 40 minutes after the unauthorized connections between the computer at the IP address ending in 117, the Mail2 server, and the Qualcomm server. Savoy determined that the computer at that IP address had been used regularly to check Heckencamp's email account, but no others. Savoy became extremely concerned because he knew that Heckenkamp had been terminated from his job at the university computer help desk two years earlier for similar unauthorized activity, and Savoy

[1] An IP address is a standard way of identifying a computer that is connected to the Internet. An IP address is comprised of four integers less than 256 separated by periods.

knew that Heckenkamp "had technical expertise to damage [the university's] system."

Although Savoy was confident that the computer that had gained the unauthorized access belonged to Heckenkamp, he checked the housing records to ensure that the IP address was assigned to Heckenkamp's dorm room. The housing department initially stated that the IP address corresponded to a different room down the hall from Heckenkamp's assigned room. The housing department acknowledged that the records could be inaccurate but stated that they would not be able to verify the location of the IP address until the next morning. In order to protect the university's server, Savoy electronically blocked the connection between IP address 117 and the Mail2 server.

After blocking the connection, Savoy contacted Rankhorn. After Savoy informed Rankhorn of the information he had found, Rankhorn told Savoy that he intended to get a warrant for the computer, but he did not ask Savoy to take any action or to commence any investigation.

Later that night, Savoy decided to check the status of the 117 computer from home because he was still concerned about the integrity of the university's system. He logged into the network and determined that the 117 computer was not attached to the network. However, Savoy was still concerned that the same computer could have "changed its identity," so he checked the networking hardware to determine if

the computer that was originally logged on at the 117 address was now logged on at a different IP address. His search confirmed that the computer was now logged on at an IP address ending in 120.

Based on this discovery, Savoy became even more concerned that the Mail2 server "security could be compromised at any time," particularly because "the intruder at this point knows that he's being investigated" and might therefore interfere with the system to cover his tracks. Savoy concluded that he needed to act that night.

Before taking action, Savoy wanted to verify that the computer logged on at 120 was the same computer that had been logged on at 117 earlier in the day. He logged into the computer, using a name and password he had discovered in his earlier investigation into the 117 computer. Savoy used a series of commands to confirm that the 120 computer was the same computer that had been logged on at 117 and to determine whether the computer still posed a risk to the university server. After approximately 15 minutes of looking only in the temporary directory, without deleting, modifying, or destroying any files, Savoy logged off of the computer.

Savoy then determined that "[the 120] machine need[ed] to get off line immediately or as soon as possible" based on "a university security need." He contacted both Rankhorn and a Detective Scheller, who worked for the university police. Savoy informed them of his discoveries and concerns. Rankhorn asked

Savoy to wait to take action because he was attempting to get a search warrant. However, Savoy felt that he needed to protect the university's system by taking the machine off line immediately. Therefore, he made the decision to coordinate with the university police to take the computer off line and to "let [the] university police coordinate with the FBI."

Together with Scheller and other university police officers, Savoy went to the room assigned to Heckenkamp.[2] When they arrived at the room, the door was ajar, and nobody was in the room. Savoy and Scheller entered the room and disconnected the network cord attaching the computer to the network. Savoy noted that the computer had a screen saver with a password, which prevented him from accessing the computer. In order to be sure that the computer he had disconnected from the network was the computer that had gained unauthorized access to the Mail2 server, Savoy wanted to run some commands on the computer. Detective Scheller located Heckenkamp, explained the situation and asked for Heckenkamp's password, which Heckenkamp voluntarily provided.

Savoy used the password to run the commands on the computer and verified that it was the computer used to gain the unauthorized access. After

---

[2] They also went to the room the housing department stated was connected to the IP address ending in 117 to ensure that those records were not correct.

Savoy confirmed that he had the right computer, Scheller advised Heckenkamp that he was not under arrest, but Scheller requested that Heckenkamp waive his Miranda rights and give a statement. Heckenkamp waived his rights in writing and answered the investigator's and detectives' questions. In addition, Heckenkamp authorized Savoy to make a copy of his hard drive for later analysis, which Savoy did. At no time did Savoy or Scheller search Heckenkamp's room. Throughout his testimony, Savoy emphasized that his actions were taken to protect the university's server rather than for law enforcement purposes.

The federal agents obtained a search warrant from the Western District of Wisconsin, which was executed the following day. Pursuant to the warrant, the agents seized the computer and searched Heckenkamp's room.

Heckenkamp was indicted in both the Northern and Southern Districts of California on multiple offenses, including counts of recklessly causing damage by intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(B). In separate orders, Judge Ware in the Northern District and Judge Jones in the Southern District denied Heckenkamp's motions to suppress the evidence gathered from (1) the remote search of his computer, (2) the image taken of his computer's

hard drive, and (3) the search conducted pursuant to the FBI's search warrant.[3]

The two cases were eventually consolidated before Judge Ware. Heckenkamp entered a conditional guilty plea to two counts of violating 18 U.S.C. § 1030(a)(5)(B), which allowed him to appeal the denials of his motions to suppress. The district court entered its judgment and commitment orders on April 28, 2005, and Heckenkamp filed a timely notice of appeal.

We review de novo both a court's denial of a motion to suppress evidence and a court's determination of whether an individual's expectation of privacy was objectively reasonable. *United States v. Bautista,* 362 F.3d 584, 588-89 (9th Cir.2004).

II

As a prerequisite to establishing the illegality of a search under the Fourth Amendment, a defendant must show that he had a reasonable expectation of privacy in the place searched. *Rakas v. Illinois,* 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). An individual has a reasonable expectation of privacy if he can "'demonstrate a subjective expectation that his activities would be private, and he [can] show that

[3] Judge Ware later reaffirmed his denial of the motion to suppress when Heckenkamp filed a renewed motion to suppress after the cases were consolidated.

his expectation was one that society is prepared to recognize as reasonable.'" *Bautista,* 362 F.3d at 589 (quoting *United States v. Nerber,* 222 F.3d 597, 599 (9th Cir.2000)). No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of warrantless government intrusion. *Rakas,* 439 U.S. at 152-153, 99 S.Ct. 421 (Powell, J., concurring). However, we have given weight to such factors as the defendant's possessory interest in the property searched or seized, *see United States v. Broadhurst,* 805 F.2d 849, 852 n. 2 (9th Cir.1986), the measures taken by the defendant to insure privacy, *see id.,* whether the materials are in a container labeled as being private, *see id.,* and the presence or absence of a right to exclude others from access, *see Bautista,* 362 F.3d at 589.

The government does not dispute that Heckenkamp had a subjective expectation of privacy in his computer and his dormitory room, and there is no doubt that Heckenkamp's subjective expectation as to the latter was legitimate and objectively reasonable. *Minnesota v. Olson,* 495 U.S. 91, 95-96, 110 S.Ct. 1684, 109 L.Ed.2d 85 (1990). We hold that he also had a legitimate, objectively reasonable expectation of privacy in his personal computer. *See United States v. Lifshitz,* 369 F.3d 173, 190 (2d Cir.2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *see also United States v. Buckner,* 473 F.3d 551, 554 n. 2 (4th Cir.2007) (recognizing a reasonable expectation of

privacy in password-protected computer files); *Trulock v. Freeh,* 275 F.3d 391, 403 (4th Cir.2001) (same).

The salient question is whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network. We conclude under the facts of this case that the act of attaching his computer to the network did not extinguish his legitimate, objectively reasonable privacy expectations.

A person's reasonable expectation of privacy may be diminished in "transmissions over the Internet or e-mail that have already arrived at the recipient." *Lifshitz,* 369 F.3d at 190. However, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer. *Leventhal v. Knapek,* 266 F.3d 64, 74 (2d Cir.2001). However, privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user. *United States v. Angevine,* 281 F.3d 1130, 1134 (10th Cir.2002); *United States v. Simons,* 206 F.3d 392, 398 (4th Cir.2000).

In the instant case, there was no announced monitoring policy on the network. To the contrary, the university's computer policy itself provides that "[i]n general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be

kept to a minimum and made only where essential to . . . protect the integrity of the University and the rights and property of the state." When examined in their entirety, university policies do not eliminate Heckenkamp's expectation of privacy in his computer. Rather, they establish limited instances in which university administrators may access his computer in order to protect the university's systems. Therefore, we must reject the government's contention that Heckenkamp had no objectively reasonable expectation of privacy in his personal computer, which was protected by a screen-saver password, located in his dormitory room, and subject to no policy allowing the university actively to monitor or audit his computer usage.

III

Although we conclude that Heckenkamp had a reasonable expectation of privacy in his personal computer, we conclude that the search of the computer was justified under the "special needs" exception to the warrant requirement. Under the special needs exception, a warrant is not required when "'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'" *Griffin v. Wisconsin,* 483 U.S. 868, 873, 107 S.Ct. 3164, 97 L.Ed.2d 709 (1987) (quoting *New Jersey v. T.L.O.,* 469 U.S. 325, 351, 105 S.Ct. 733, 83 L.Ed.2d 720 (1985) (Blackmun, J., concurring in the judgment)). If a court determines that such conditions exist, it will "assess the constitutionality of

the search by balancing the need to search against the intrusiveness of the search." *Henderson v. City of Simi Valley,* 305 F.3d 1052, 1059 (9th Cir.2002) (citing *Ferguson v. City of Charleston,* 532 U.S. 67, 78, 121 S.Ct. 1281, 149 L.Ed.2d 205 (2001)).

A

Here, Savoy provided extensive testimony that he was acting to secure the Mail2 server, and that his actions were not motivated by a need to collect evidence for law enforcement purposes or at the request of law enforcement agents. This undisputed evidence supports Judge Jones's conclusion that the special needs exception applied. The integrity and security of the campus e-mail system was in jeopardy. Although Savoy was aware that the FBI was also investigating the use of a computer on the university network to hack into the Qualcomm system, his actions were not taken for law enforcement purposes. Not only is there no evidence that Savoy was acting at the behest of law enforcement, but also the record indicates that Savoy was acting contrary to law enforcement requests that he delay action.

Under these circumstances, a search warrant was not necessary because Savoy was acting purely within the scope of his role as a system administrator. Under the university's policies, to which Heckenkamp assented when he connected his computer to the university's network, Savoy was authorized to "rectif[y] emergency situations that threaten the integrity

of campus computer or communication systems[,] provided that use of accessed files is limited solely to maintaining or safeguarding the system." Savoy discovered through his examination of the network logs, in which Heckenkamp had no reasonable expectation of privacy, that the computer that he had earlier blocked from the network was now operating from a different IP address, which itself was a violation of the university's network policies.

This discovery, together with Savoy's earlier discovery that the computer had gained root access to the university's Mail2 server, created a situation in which Savoy needed to act immediately to protect the system. Although he was aware that the FBI was already seeking a warrant to search Heckenkamp's computer in order to serve the FBI's law enforcement needs, Savoy believed that the university's separate security interests required immediate action. Just as requiring a warrant to investigate potential student drug use would disrupt operation of a high school, *see T.L.O.*, 469 U.S. at 352-53, 105 S.Ct. 733 (Blackmun, J., concurring in the judgment), requiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function. Moreover, Savoy and the other network administrators generally do not have the same type of "adversarial relationship" with the university's network users as law enforcement officers generally have with criminal suspects. 469 U.S. at 349-50, 105 S.Ct. 733 (Powell, J., concurring).

The district court was entirely correct in holding that the special needs exception applied.

B

Once a court determines that the special needs doctrine applies to a search, it must "assess the constitutionality of the search by balancing the need to search against the intrusiveness of the search." *Henderson,* 305 F.3d at 1059 (citing *Ferguson,* 532 U.S. at 78, 121 S.Ct. 1281). The factors considered are the subject of the search's privacy interest, the government's interests in performing the search, and the scope of the intrusion. *See id.* at 1059-60.

Here, although Heckenkamp had a subjectively real and objectively reasonable expectation of privacy in his computer, the university's interest in maintaining the security of its network provided a compelling government interest in determining the source of the unauthorized intrusion into sensitive files. The remote search of the computer was remarkably limited given the circumstances. Savoy did not view, delete, or modify any of the actual files on the computer; he was only logged into the computer for 15 minutes; and he sought only to verify that the same computer that had been connected at the 117 IP address was now connected at the 120 IP address. Here, as in *Henderson,*"the government interest served[] and the relative unobtrusiveness of the search" lead to a conclusion that the remote search was not unconstitutional. *Id.* at 1061.

The district court did not err in denying the motion to suppress the evidence obtained through the remote search of the computer.

IV

The district court also did not err in denying the motion to suppress evidence obtained during the searches of Heckenkamp's room. Assuming, without deciding, that Savoy and the university police violated Heckenkamp's Fourth Amendment rights when they entered his dormitory room for nonlaw-enforcement purposes, the evidence obtained through the search was nonetheless admissible under the independent source exception to the exclusionary rule.

Under the independent source exception, "'information which is received through an illegal source is considered to be cleanly obtained when it arrives through an independent source.'" *Murray v. United States,* 487 U.S. 533, 538-39, 108 S.Ct. 2529, 101 L.Ed.2d 472, (1988) (quoting *United States v. Silvestri,* 787 F.2d 736, 739 (1st Cir.1986)). Therefore, we have held that "'[t]he mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant.'" *United States v. Reed,* 15 F.3d 928, 933 (9th Cir.1994) (quoting *United States v. Vasey,* 834 F.2d 782, 788 (9th Cir.1987)). In order to determine whether evidence obtained through a tainted warrant is admissible, "[a] reviewing court should excise the tainted evidence and determine whether the remaining untainted evidence

would provide a neutral magistrate with probable cause to issue a warrant." *Id.* (quoting *Vasey,* 834 F.2d at 788).

Here, even without the evidence gathered through the allegedly improper search, there is sufficient information in the affidavit to establish probable cause. The affidavit recited evidence that the server intrusion had been tracked "to a campus dormitory room computer belonging to Jerome T. Heckenkamp"; that "[t]he computer is in Room 107, Noyes House, Adams Hall on the University of Wisconsin-Madison"; and that "Heckenkamp previously had a disciplinary action in the past for unauthorized computer access to a University of Wisconsin system." This was sufficient evidence to obtain the warrant to search "Room 107, Noyes House, Adams Hall."

V

Although Heckenkamp had a reasonable expectation of privacy in his personal computer, a limited warrantless remote search of the computer was justified under the special needs exception to the warrant requirement. The subsequent search of his dorm room was justified, based on information obtained by means independent of the university search of the room. Therefore, the district courts properly denied the suppression motions.

The judgment of the district court is **AFFIRMED.**

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. JEROME T. HECKENKAMP, Defendant-Appellant.	No. 05-10322 D.C. No. CR-03-20041-JW ORDER

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. JEROME T. HECKENKAMP, Defendant-Appellant.	No. 05-10323 D.C. No. CR-00-20355-JW (Filed Jul. 19, 2007)

Before: CANBY, HAWKINS, and THOMAS, Circuit Judges.

The panel has voted to deny the petition for rehearing. Judges Hawkins and Thomas voted to reject the suggestion for rehearing en banc, and Judge Canby so recommended.

The full court has been advised of the suggestion for rehearing en banc, and no judge of the court has requested a vote on the suggestion for rehearing en banc. Fed. R. App. P. 35(b).

The petition for rehearing is denied and the suggestion for rehearing en banc is rejected.